



National Aeronautics and
Space Administration
Washington, DC 20546

Procurement Notice

PN 97-75
July 26, 2002

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

BACKGROUND: An interim rule was published in the Federal Register on July 12, 2001, and incorporated into the NFS by Procurement Notice 97-63. This interim rule revised the clause at 1852.204-76, Security Requirements for Unclassified Information Technology Resources. Procurement Information Circular (PIC) 02-04 established a date of April 30, 2002, for incorporation into applicable contracts of the July 2001 version of the clause unless the contract already contained the July 2000 version of the clause. This PN incorporates the final rule which adopted the interim rule published earlier with changes. The primary change is to the screening requirements contained in the paragraph (d)(3)(i) of 1852.204-76. The interim rule personnel-screening process waived provisions requiring financial and medical information. As a result of the events of September 11, 2001, increased emphasis has been placed on security. Due to the new emphasis on security, OPM will no longer perform National Agency Checks on contractor employees who do not provide financial and medical information required currently by Standard Form 85P. Thus, the final rule reinstates the requirement for financial and medical information for employees going through the screening process. Employee information submitted now must include related financial and medical information as required by the Government or the equivalent if screening is performed by the contractor.

ACTION REQUIRED BY CONTRACTING OFFICERS:

A. All solicitations and contracts issued after July 26, 2002, requiring the use of the clause at 1852.204-76, Security Requirements for Unclassified Information Technology Resources, must include the revised clause dated "July 2002."

B. Solicitations issued before, July 26, 2002, should be amended to include the revised clause if including the clause would not unduly delay the acquisition.

C. Amend existing contracts requiring screening based on a risk level of IT-1 (highest level of risk) that contain the clause dated "July 2001" to incorporate the revised clause dated "July 2002." Existing contracts requiring screening based on risk levels of IT-2 and IT-3 do not require modification.

CLAUSE CHANGES: This PN revises the clause at 1852.204-76, Security Requirements for Unclassified Information Technology Resources, by deleting the parenthetical statement "(Information regarding financial record, question 22, and the Authorization for Release of Medical Information are not applicable.)" in paragraph (d)(3)(i).

PARTS AFFECTED: Changes are made in Parts 1804 and 1852.

REPLACEMENT PAGES: You may use the enclosed pages to replace 4:3, 4:4, 4:4.1 (added), 52:7, 52:8, 52-91 and 52-92.

TYPE OF RULE AND PUBLICATION DATE: This PN was published as a final rule in the Federal Register (67 FR 48814-48815) on July 26, 2002.

HEADQUARTERS CONTACT: Karl Beisel, Code HC, (202) 358-0416, e-mail: kbeisel@hq.nasa.gov.

R. Scott Thompson
Director, Contract Management Division

Enclosures

4:

1804.7401	Definitions.
1804.7402	Policy
1804.7403	Procedures.
1804.7404	Solicitation provisions and contract clauses.

PART 1804

ADMINISTRATIVE MATTERS

Subpart 1804.1--Contract Execution

1804.103 Contract clause.

The contracting officer shall include the clause at FAR 52.204-1, Approval of Contract, in solicitations, contracts, and supplemental agreements that require higher level approval. For actions requiring Headquarters approval, insert "NASA Assistant Administrator for Procurement" in the clause's blank space.

1804.170 Contract effective date.

(a) "**Contract effective date**" means the date agreed upon by the parties for beginning the period of performance under the contract. In no case shall the effective date precede the date on which the contracting officer or designated higher approval authority signs the document.

(b) Costs incurred before the contract effective date are unallowable unless they qualify as precontract costs (see FAR 31.205-32) and the clause prescribed at 1831.205-70 is used.

Subpart 1804.2--Contract Distribution

1804.202 Agency distribution requirements.

In addition to the requirements in FAR 4.201, the contracting officer shall distribute one copy of each R&D contract, including the Statement of Work, to the NASA Center for AeroSpace Information (CASI), Attention: Document Processing Section, 7121 Standard Drive, Hanover, MD 21076-1320.

1804.203 Taxpayer identification information.

Instead of using the last page of the contract to provide the information listed in FAR 4.203, NASA installations may allow contracting officers to use a different distribution method, such as annotating the cover page of the payment office copy of the contract.

Subpart 1804.4--Safeguarding Classified Information Within Industry

1804.402 General.

(b) NASA security policies and procedures are prescribed in NPD 1600.2A, NASA Security Policy; NPG 1600.6A, Communications Security Procedures and Guidelines; NPG 1620.1, Security Procedures and Guidelines; NPG 2810.1 and NPD 2810.1 Security of Information Technology.

4:

1804.404-70 Contract clause.

The contracting officer shall insert the clause at 1852.204-75, Security Classification Requirements, in solicitations and contracts if work to be performed will require security clearances. This clause may be modified to add instructions for obtaining security clearances and access to security areas that are applicable to the particular acquisition and installation.

1804.470 Security requirements for unclassified information technology resources.

1804.470-1 Scope.

This section implements NASA's acquisition-related aspects of Federal policies for assuring the security of unclassified automated information resources. Federal policies include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.), the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.), Public Law 106-398, section 1061, Government Information Security Reform, OMB Circular A-130, Management of Federal Information Resources, and the National Institute of Standards and Technology security guidance and standards.

1804.470-2 Policy.

(a) NASA policies and procedures on security for automated information technology are prescribed in NPD 2810.1, Security of Information Technology, and in NPG 2810.1, Security of Information Technology. The provision of information technology (IT) security in accordance with these policies and procedures, is required in all contracts that include IT resources or services in which a contractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

- (1) Computer control of spacecraft, satellites, or aircraft or their payloads;
- (2) Acquisition, transmission or analysis of data owned by NASA with significant replacement costs should the contractor's copy be corrupted; and
- (3) Access to NASA networks or computers at a level beyond that granted the general public, e.g. bypassing a firewall.

(b) The contractor must not use or redistribute any NASA information processed, stored, or transmitted by the contractor except as specified in the contract.

1804.470-3 Security plan for unclassified Federal Information Technology systems.

(a) The requiring activity with the concurrence of the Center Chief Information Officer (CIO), and the Center Information Technology (IT) Security Manager, must determine whether an IT Security Plan for unclassified information is required.

(b) IT security plans must demonstrate a thorough understanding of NPG 2810.1 and NPD 2810.1 and must include, as a minimum, the security measures and program safeguards planned to ensure that the information technology resources acquired and used by contractor and subcontractor personnel --

- (1) Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

4:

(2) Can maintain the continuity of automated information support for NASA missions, programs, and functions;

PROCUREMENT NOTICE (PN) 97-75 REPLACEMENT PAGE

4:4.1

(3) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy;

(4) Have appropriate technical, personnel, administrative, environmental, and access safeguards;

1852.204-76 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 1804.470-4, insert a clause substantially as follows:

**SECURITY REQUIREMENTS FOR UNCLASSIFIED
INFORMATION TECHNOLOGY RESOURCES
(JULY 2002)**

(a) The Contractor shall be responsible for Information Technology security for all systems connected to a NASA network or operated by the Contractor for NASA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

- (1) Computer control of spacecraft, satellites, or aircraft or their payloads;
- (2) Acquisition, transmission or analysis of data owned by NASA with significant replacement cost should the contractor's copy be corrupted; and
- (3) Access to NASA networks or computers at a level beyond that granted the general public, e.g. bypassing a firewall.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.) and the Government Information Security Reform Act of 2000. The plan shall meet IT security requirements in accordance with Federal and NASA policies and procedures that include, but are not limited to:

- (1) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;
- (2) NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology; and
- (3) Chapter 3 of NPG 1620.1, NASA Security Procedures and Guidelines.

(c) Within ____ days after contract award, the contractor shall submit for NASA approval an IT Security Plan. This plan must be consistent with and further detail the approach contained in the offeror's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(d)(1) Contractor personnel requiring privileged access or limited privileged access to systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPG 2810.1, Section 4.5; NPG 1620.1, Chapter 3; and paragraph (d)(2) of this clause. Those Contractor personnel with non-privileged access do not require personnel screening. NASA shall provide screening using standard personnel screening National Agency Check (NAC) forms listed in paragraph (d)(3) of this clause, unless contractor screening in accordance with paragraph (d)(4) is approved. The Contractor shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after contract award or assignment of an individual to a position requiring screening. The forms may be obtained from the CCS. At the option of the government, interim access may be granted pending completion of the NAC.

(2) Guidance for selecting the appropriate level of screening is based on the risk of adverse impact to NASA missions. NASA defines three levels of risk for which screening is required

(IT-1 has the highest level of risk):

(i) **IT-1** -- Individuals having privileged access or limited privileged access to systems whose misuse can cause very serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of spacecraft, satellites or aircraft.

(ii) **IT-2** -- Individuals having privileged access or limited privileged access to systems whose misuse can cause serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of payloads on spacecraft, satellites or aircraft; and those that contain the primary copy of "level 1" data whose cost to replace exceeds one million dollars.

(iii) **IT-3** -- Individuals having privileged access or limited privileged access to systems whose misuse can cause significant adverse impact to NASA missions. These systems include, for example, those that interconnect with a NASA network in a way that exceeds access by the general public, such as bypassing firewalls; and systems operated by the contractor for NASA whose function or data has substantial cost to replace, even if these systems are not interconnected with a NASA network.

(3) Screening for individuals shall employ forms appropriate for the level of risk as follows:

(i) IT-1: Fingerprint Card (FC) 258 and Standard Form (SF) 85P, Questionnaire for Public Trust Positions;

(ii) IT-2: FC 258 and SF 85, Questionnaire for Non-Sensitive Positions; and

(iii) IT-3: NASA Form 531, Name Check, and FC 258.

(4) The Contracting Officer may allow the Contractor to conduct its own screening of individuals requiring privileged access or limited privileged access provided the Contractor can demonstrate that the procedures used by the Contractor are equivalent to NASA's personnel screening procedures. As used here, equivalent includes a check for criminal history, as would be conducted by NASA, and completion of a questionnaire covering the same information as would be required by NASA.

(5) Screening of contractor personnel may be waived by the Contracting Officer for those individuals who have proof of --

(i) Current or recent national security clearances (within last three years);

(ii) Screening conducted by NASA within last three years; or

(iii) Screening conducted by the Contractor, within last three years, that is equivalent to the NASA personnel screening procedures as approved by the Contracting Officer under paragraph (d)(4) of this clause.

(e) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices in accordance with NPG 2810.1, Section 4.3 requirements. The contractor may use web-based training available from NASA to meet this requirement.